

DIALOG(R)File 351:Derwent WPI
(c) 2001 Derwent Info Ltd. All rts. reserv.

011464376 **Image available**
WPI Acc No: 1997-442283/*199741*
XRPX Acc No: N97-368190

Video input unit e.g. digital camera - has codec that forms digital
signature for identifying digital data, based on either confidential
information inherent to unit or to external device connected to unit

Patent Assignee: CANON KK (CANO)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 9200730	A	19970731	JP 963603	A	19960112	199741 B

Priority Applications (No Type Date): JP 963603 A 19960112

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 9200730	A		12	H04N-007/167	

Abstract (Basic): JP 9200730 A

The input unit receives an image data and transforms it to a digital data. Based on a confidential information inherent to an external device connected to the unit, or a confidential information inherent to the unit, a codec (C-CODEC) forms a digital signature used for identifying the digital data. An example of the confidential information is a secret key used by a digital signature system of open key encryption type.

ADVANTAGE - Raises alteration proof capacity of digital data, thus extending application range.

Dwg.1/6

Title Terms: VIDEO; INPUT; UNIT; DIGITAL; CAMERA; CODEC; FORM; DIGITAL;
SIGNATURE; IDENTIFY; DIGITAL; DATA; BASED; CONFIDE; INFORMATION; INHERENT
; UNIT; EXTERNAL; DEVICE; CONNECT; UNIT

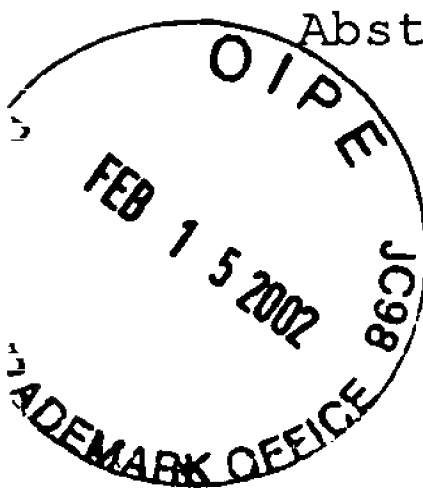
Derwent Class: P85; U21; W01; W02; W04

International Patent Class (Main): H04N-007/167

International Patent Class (Additional): G09C-001/00; H03M-007/30;
H04L-009/32; H04N-005/91

File Segment: EPI; EngPI

Manual Codes (EPI/S-X): U21-A05A2; W01-A05; W02-F05A1; W02-F10N1; W04-F01L1



RECEIVED
FEB 25 2002
Technology Center 2600

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-200730

(43) 公開日 平成9年(1997)7月31日

(51) Int.Cl. ⁸	識別記号	序内整理番号	F I	技術表示箇所
H 0 4 N 7/167			H 0 4 N 7/167	
G 0 9 C 1/00	6 4 0	7259-5 J	G 0 9 C 1/00	6 4 0 A
		7259-5 J		6 4 0 D
H 0 4 L 9/32		9382-5 K	H 0 3 M 7/30	Z
H 0 4 N 5/91			H 0 4 L 9/00	6 7 5 A
審査請求 未請求 請求項の数 8 O L (全 12 頁) 最終頁に続く				

(21) 出願番号 特願平8-3603

(22) 出願日 平成8年(1996)1月12日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 大石 和臣

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

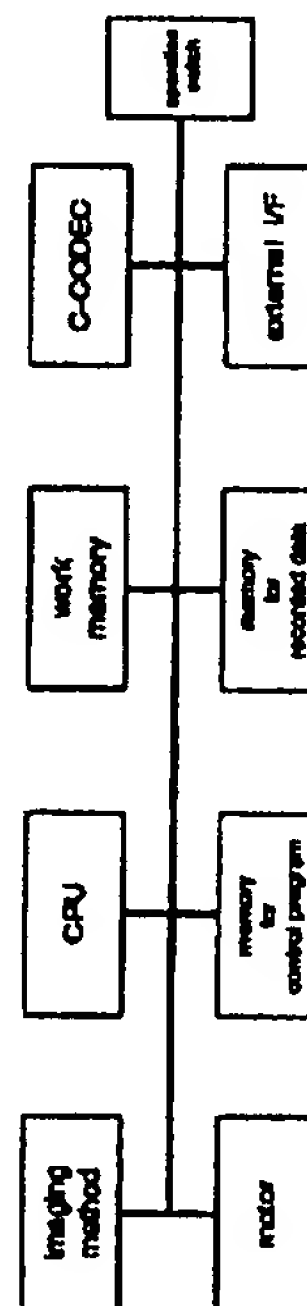
(74) 代理人 弁理士 園分 孝悦

(54) 【発明の名称】 映像入力装置および映像入力システム

(57) 【要約】

【課題】 形成されたデジタル映像データの正当性を
認証することを可能にする映像入力装置を提供する。

【解決手段】 映像を入力してデジタル変換する映像
入力装置において、上記映像入力装置に固有の秘密情報
(例えば、公開鍵暗号系のデジタル署名方式で使用さ
れる秘密鍵)と、上記デジタル変換された映像データ
とに基づき、上記映像データを識別するデジタル署名
を生成するデジタル署名生成部C-CODECを設け、形成
した映像データに対して、映像入力装置だけが生成でき
るデジタル署名を求め、映像データとそれに対応する
デジタル署名とを映像入力装置の出力データとすること
により、ある映像データを形成する映像入力装置以外
のものがそれに対応するデジタル署名を生成できない
ようにするとともに、出力データに対して改ざんや偽造
がなされたときは、それを検出できるようにする。



【特許請求の範囲】

【請求項1】 映像を入力してデジタル・データに変換する映像入力装置において、

上記映像入力装置に固有の秘密情報および上記映像入力装置に接続される外部装置に固有の秘密情報の少なくとも一方の情報と、上記変換されたデジタル・データとに基づき、所定の演算を実行し、上記デジタル・データを識別する情報を生成する手段を有することを特徴とする映像入力装置。

【請求項2】 上記所定の演算として、公開鍵暗号系を用いるデジタル署名方式の演算を実行することを特徴とする請求項1に記載の映像入力装置。

【請求項3】 上記所定の演算を、上記映像入力装置の内部および上記映像入力装置に接続される外部装置の内部の少なくとも一方において実行することを特徴とする請求項1または2に記載の映像入力装置。

【請求項4】 上記映像入力装置に入力され変換されたデジタル・データに対して圧縮変換を行なう手段と、上記圧縮変換された結果のデータに対して上記所定の演算を行なうように制御する手段とを有することを特徴とする請求項1～3の何れか1項に記載の映像入力装置。

【請求項5】 映像を入力してデジタル・データに変換する映像入力システムにおいて、
上記映像入力システムに固有の秘密情報および上記映像入力システムに接続される外部装置に固有の秘密情報の少なくとも一方の情報と、上記変換されたデジタル・データとに基づき、所定の演算を実行し、上記デジタル・データを識別する情報を生成する手段と、
上記デジタル・データを識別する情報を用いて、上記生成されたデジタル・データが確かに上記映像入力システムで生成されたものかどうかを検証する手段とを有することを特徴とする映像入力システム。

【請求項6】 上記所定の演算として、公開鍵暗号系を用いるデジタル署名方式の演算を実行することを特徴とする請求項5に記載の映像入力システム。

【請求項7】 上記所定の演算を、上記映像入力システムの内部および上記映像入力システムに接続される外部装置の内部の少なくとも一方において実行することを特徴とする請求項5または6に記載の映像入力システム。

【請求項8】 上記映像入力システムに入力され変換されたデジタル・データに対して圧縮変換を行なう手段と、
上記圧縮変換された結果のデータに対して上記所定の演算を行なうように制御する手段とを有することを特徴とする請求項5～7の何れか1項に記載の映像入力システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、映像入力装置および映像入力システムに関する。

【0002】

【従来の技術】 映像を入力してデジタルの映像データを形成する映像入力装置や映像入力システムは、映像データの高精細化および高画質化と、装置あるいはシステムの低コスト化とが追求されることが一般的である。そのために、高解像度の入力デバイスや効率の良い符号化、および小型化のための技術等が広範に研究開発されている。

【0003】 これに対し、形成されたデジタルの映像データが確かにその映像入力装置あるいは映像入力システムで形成されたことを保証する技術を機能として組み込むことは、従来あまり考えられていなかった。

【0004】

【発明が解決しようとする課題】 アナログの映像入力装置では、形成される映像はアナログ・データであるため、その映像データの改ざんあるいは偽造を行うためには特殊な知識、能力等が必要であり、結果的に改ざんや偽造が成功することは少なかった。これに対して、デジタルの映像データの場合は、比較的容易に改ざんや偽造が行なわれ得るため、映像データの信憑性が低いという問題があった。

【0005】 例えば、銀塩写真のネガ・フィルムに記憶されている映像は、銀塩分子により構成されているため、これを見破って改ざんや偽造を行うことは困難である。これに対して、デジタル・データで表現されている映像は、0と1のビット列から構成されているため、コンピュータを用いて改ざんや偽造が行なわれやすい。したがって、デジタルの映像データは、事実の証拠としての証明能力が小さい、すなわち信憑性が低いと言え、用途が限定される恐れがある。

【0006】 本発明はこのような問題を解決するために成されたものであり、形成されたデジタル映像データの正当性を認証することができるようにした映像入力装置および映像入力システムを提供することを目的とする。

【0007】

【課題を解決するための手段】 本発明の映像入力装置およびシステムは、デジタル・データの正当性を保証するための技術であるデジタル署名を応用する。デジタル署名とは、岡本栄司著の暗号理論入門（共立出版株式会社）によれば、「メッセージや情報の作成者が確かにそれらを作成したことを示す」ものである。つまり、ユーザや、計算機等の通信または計算処理を行なう主体（エンティティと呼ぶ）があるデジタル・データを認めたときに、その事実を示す証拠として用いられるデジタル・データである。

【0008】 本発明の映像入力装置は、形成したデジタルの映像データに対して、映像入力装置だけが生成できるデジタル署名を求め、映像データ自体とそれに対応するデジタル署名とを映像入力装置の出力データと

する。そして、本発明の映像入力システムにおいて、上記出力データを受け取ったエンティティは、映像データとデジタル署名との対応関係が正しく成り立つかどうかを確認し、正しい対応関係が認められないデータは正当ではないとする。

【0009】上述の手段により、あるデジタル映像データを形成する映像入力装置以外のものは、その映像データに対応するデジタル署名を生成することはできず、かつ、出力データに対して改ざんや偽造がなされたときは、それを検出することが可能になる。したがって、その映像データが確かにその映像入力装置で生成されたものだということが保証することが可能になり、デジタル映像データに事実の証拠としての証明能力を与えることができる。

【0010】

【発明の実施の形態】

〔第1の実施形態〕本実施形態では、デジタル署名のアルゴリズムとして公開鍵暗号を用い、映像入力装置の内部に固有の秘密情報として公開鍵暗号を有する場合について説明する。ただし、これは1つの例であり、公開鍵暗号を用いるデジタル署名アルゴリズムの代わりに、元情報と秘密情報とに基づいて元情報を識別する情報を生成する手段を有するものは本実施形態に全て含まれる。

【0011】以下では、最初に公開鍵暗号について説明する。次に、映像入力装置の構成について説明し、公開鍵暗号を用いたデジタル署名を適用した本実施形態の映像入力装置がデジタル署名を生成するときの具体的な手続きを述べる。最後に、映像入力システムの機能の一部として、そのデジタル署名を検証するときの具体的な手続きについて説明する。

【0012】公開鍵暗号

公開鍵暗号とは、暗号鍵と復号鍵とが異なり、暗号鍵を公開するとともに復号鍵を秘密に保持する暗号方式である。公開鍵暗号は、送られてきた通信文の送信者が偽者でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現でき、デジタル署名を実現する有力な技術だと考えられている。

【0013】例えば、通信文Mに対して、公開の暗号鍵 k_p を用いて行う暗号化操作を $E(k_p, M)$ とし、秘密の復号鍵 k_s を用いて行う復号操作を $D(k_s, M)$ とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

(1) 暗号鍵 k_p が与えられたとき、暗号化操作 $E(k_p, M)$ の計算は容易である。また、復号鍵 k_s が与えられたとき、復号操作 $D(k_s, M)$ の計算は容易である。

(2) もしユーザが復号鍵 k_s を知らないなら、暗号鍵 k_p と暗号化操作 $E(k_p, M)$ の計算手順と $C = E(k_p, M)$ とを知っていても、通信文Mを決定するこ

とは計算量の点で困難である。

【0014】次に、上記(1)、(2)の条件に加えて、次の(3)の条件が成立することにより秘密通信機能を実現できる。

(3) 全ての通信文(平文)Mに対し暗号化操作 $E(k_p, M)$ が定義でき、

$$D(k_s, E(k_p, M)) = M$$

が成立する。つまり、暗号鍵 k_p は公開されているため誰もが暗号化操作 $E(k_p, M)$ の計算を行うことができるが、 $D(k_s, E(k_p, M))$ の計算をして通信文Mを得ることができるのは復号鍵 k_s を持っている本人だけである。

【0015】一方、上記(1)、(2)の条件に加えて、次の(4)の条件が成立することにより認証機能を実現できる。

(4) 全ての通信文(平文)Mに対し復号操作D

(k_s, M) が定義でき、

$$E(k_p, D(k_s, M)) = M$$

が成立する。

【0016】つまり、復号操作 $D(k_s, M)$ の計算ができるのは復号鍵 k_s を持っている本人のみであり、他の人が偽の秘密鍵 k_s' を用いて $D(k_s', M)$ の計算を行い、復号鍵 k_s を持っている本人になりすましたとしても、

$$E(k_p, D(k_s', M)) \neq M$$

なので、受信者は受けとった情報が不正なものであることを認識できる。また、 $D(k_s, M)$ の値が改ざんされても $E(k_p, D(k_s, M)')$ $\neq M$ となり、受信者は受けとった情報が不正なものであることを確認できる。この復号操作 $D(k_s, M)$ を通信文Mに対するデジタル署名と呼ぶ。

【0017】以下に、代表的な公開鍵暗号方式を挙げる。上述の秘密通信と認証通信とを行うことができる方式として、RSA暗号(R.L.Rivest, A.Shamir and L.Adleman: "A method of obtaining digital signatures and public key cryptosystems", Comm. of ACM 1977)、R暗号(M.Rabin: "Digitalized signatures and public-key cryptosystems", MIT/LCS/TR-212, Technical Report MIT, 1979)、W暗号(H.C.Williams: "A modification of the RSA public-key encryption procedure", IEEE Trans. Inf. Theory, IT-26, 6, 1980)、MI暗号(松本, 今井: "公開鍵暗号系の新しいアルゴリズム", 信学技報, IT82-84, 1982; T.Matsumoto and H.Imai: "A class of asymmetric cryptosystems based on polynomials over finite rings", IEEE International Symp. on Information Theory, 1983)などがある。

【0018】また、秘密通信のみができる方式として、MH暗号(R.C.Merkle and M.E.Hellman: "Hiding in information and signatures in trapdoor knapsacks", IEEE Trans. Inf. Theory, IT-24, 5, 1987)、GS信号

(A. Shamir and R. E. Zippel: "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans. Inf. Theory, IT-26, 3, 1980)、C R暗号(B. Chor and R. L. Rivest: "A knapsack type public key cryptosystems based on arithmetic in finite field", Proc. Crypto 84)、M暗号(R. J. McEliece: "A public-key cryptosystem based on algebraic coding theory" DSN Progress Rpt., Jet Propulsion Lab., 1978)、E暗号(T. E. ElGamal: "A Public key cryptosystem and a signature scheme based on discrete logarithm", Proc. Crypto 84, 1984)、T暗号(辻井重男: "行列分解を利用した公開鍵暗号の一方式", 信学技報, IT85-12, 1985)などがある。

【0019】さらに、認証通信のみができる方式として、S暗号(A. Shamir: "A fast signature scheme", Report MIT/LCS/TM-107, MIT laboratory for computer science, Cambridge, Mass., 1978)、L暗号(K. Lieberherr: "Uniform complexity and digital signature", Lecture Notes in Computer Science 115 Automata, Language and programming, Eighth Colloquium Acre, Israel, 1981)、GMY暗号(S. Goldwasser, S. Micali and A. Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983)、GMR暗号(S. Goldwasser, S. Micali and R. L. Rivest: "A 'paradoxical' solution to the signature problem", ACM Symp. on Foundation of Computer Science, 1984)、OSS暗号(H. Ong, C. P. Schnorr and A. Shamir.: "An efficient signature scheme based on quadratic equation", ACM Symp. on Theory of Computing 1984)、OS暗号(岡本、白井: "多項式演算によるデジタル署名方式、信学論(D)、J68-D, 5, 1985; T. Okamoto and A. Shirai: "A fast signature scheme based on quadratic inequalities", IEEE Symp. on Theory of Computing, 1984)などがある。

【0020】映像入力装置の構成

次に、上記のような公開鍵暗号を用いたデジタル署名を適用した本実施形態の映像入力装置について、図1を用いて説明する。図1に示した四角の各ブロックは機能別の構成要素であり、それらを結ぶ線は制御バス及びデータバスを表す。imaging methodは撮像部であり、対象となる被写体を撮影して電気信号に変換し、適当な信号処理、A/D変換処理、画像処理、情報源符号化処理等を行ない、デジタル・データを出力する。

【0021】CPUは中央演算装置であり、memory for control programに記憶されている制御ソフトウェアに従い、所定の計算および制御を行なう。上記memory for control programはメモリ部であり、上記制御ソフトウェアを記憶する。work memoryはメモリ部であり、CPUが計算を行なうための作業用に使われる。operation switchは操作部であり、装置を使用するユーザが種々の

指示を入力するためのものである。

【0022】motorは機構動作部であり、CPUの制御に応じて図示しない機械的な動作機構を制御する。memory for recorded dataはメモリ部であり、本装置が出力する映像データあるいはその一部を記録する。external I/Fは、コンピュータあるいは着脱可能なメモリ等の外部装置とのインターフェイス部であり、映像データや制御ソフトウェア等を上記外部装置との間で通信する。C-CODECはデジタル署名生成部であり、入力されたデジタル・データに対するデジタル署名を生成する。

【0023】このような構成において、映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、操作者は、操作部operation switchからその指示を入力する。CPUは、その撮影指示と、メモリ部memory for control programに記憶されている制御ソフトウェアとに従って、撮像部imaging methodや機構動作部motorを制御して対象を撮影し、その撮影により形成された映像のデジタル・データをデジタル署名生成部C-CODECに入力する。デジタル署名生成部C-CODECは、入力されたデジタル・データに対応するデジタル署名を生成する。

【0024】そして、このようにして形成された映像データとそれに対応するデジタル署名は、操作者からの指示に応じて、メモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影して形成されたデジタル・データが一度メモリ部memory for recorded dataに記録された後にデジタル署名生成部C-CODECに入力されることもあり得る。

【0025】次に、以上のような映像入力装置に対して公開鍵暗号を用いるデジタル署名を適用して、装置内に固有の秘密情報として秘密鍵を有する場合について説明する。

【0026】本実施形態による映像入力装置の秘密鍵(復号鍵)を $s_{k_{ca}}$ 、デジタル署名生成アルゴリズムを D_{ca} 、公開鍵(暗号鍵)を $p_{k_{ca}}$ 、デジタル署名検証アルゴリズムを E_{ca} とする。秘密鍵 $s_{k_{ca}}$ とデジタル署名生成アルゴリズム D_{ca} は、デジタル署名生成部C-CODECの内部に記憶されている。また、公開鍵 $p_{k_{ca}}$ とデジタル署名検証アルゴリズム E_{ca} は、少なくともデータの正当性を確認するエンティティ(検証者と呼ぶ)には知られている。

【0027】上記のような映像入力装置において、デジタル署名が生成されるとき具体的な手続きは次のようになる。

【0028】デジタル署名生成

本実施形態の映像入力装置で形成されたデジタル映像データIは、デジタル署名生成部C-CODECに入力される。デジタル署名生成部C-CODECは、その内部に記憶

されている秘密鍵 sk_{can} とデジタル署名生成アルゴリズム D_{can} とを用いて $D_{can}(sk_{can}, I)$ を計算し、デジタル署名として出力する。そして、このようにして得られる映像データ I とデジタル署名 $D_{can}(sk_{can}, I)$ は、メモリ部 memory for recorded data に記録されるか、外部装置とのインターフェイス external I/F を介して外部装置に送られるか、あるいはその両方が行なわれる。

【0029】また、映像データとそれに対応するデジタル署名とが確かに上記の映像入力装置によって入力された映像であるか否かを検証する具体的な手続きは、以下になる。なお、映像入力装置に加えて以下に述べる検証の手続きも含めたシステム全体を、映像入力システムという。

【0030】デジタル署名検証

映像データ I' とデジタル署名 $D'_{can}(sk_{can}, I)$ を受け取った検証者は、公開鍵 pk_{can} とデジタル署名検証アルゴリズム E_{can} とを用いて、 $I' = E_{can}(pk_{can}, D'_{can}(sk_{can}, I))$ が成り立つかどうかを確認する。

【0031】ここで、上式が成立した場合は、受け取った映像データ I' は上記映像入力装置で撮影された映像データ I である。一方、上式が成立しない場合は、受け取った映像データ I' が上記映像入力装置で撮影された映像データ I ではない映像になっている。すなわち、 $D'_{can}(sk_{can}, I)$ の値が $D_{can}(sk_{can}, I)$ の値とは異なる、あるいは映像データ I' とデジタル署名 $D'_{can}(sk_{can}, I)$ との両方が異なる、のいずれかの場合であり、上記装置で撮影、形成された映像データではないと判断することができる。

【0032】〔第2の実施形態〕本実施形態では、デジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置に接続される外部装置に固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図1を用いて説明する。

【0033】本実施形態においては、次に述べる外部装置としての携帯装置（図示せず）に収められている秘密鍵を sk_{aan} 、デジタル署名生成アルゴリズムを D_{aan} とし、対応する公開鍵を pk_{aan} 、デジタル署名検証アルゴリズムを E_{aan} とする。また、上記携帯装置は、携帯型の情報処理装置であり、撮影の際には、外部装置とのインターフェイス external I/F を介して映像入力装置に接続されるものである。映像データの正当性を確認するエンティティ（検証者と呼ぶ）は、デジタル署名検証アルゴリズム E_{aan} と公開鍵 pk_{aan} を知っている。

【0034】映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、上記携帯装置は映像入力装置内の外部装置とのインターフェイス external I/F に接続され、撮影者は、

操作部 operation switch から撮影の指示を入力する。CPU は、その撮影指示と、メモリ部 memory for control program に記憶されている制御ソフトウェアに従って、撮像部 imaging method や機構動作部 motor を制御して対象を撮影し、それにより得られる映像のデジタルデータをデジタル署名生成部 C-CODEC に入力する。

【0035】CPU と携帯装置は、外部装置とのインターフェイス external I/F を介して通信する。これにより、デジタル署名生成部 C-CODEC は、携帯装置に記憶されている秘密鍵 sk_{aan} とデジタル署名生成アルゴリズム D_{aan} とを得て、これらの情報を用いて、上記撮影して形成された映像データに対するデジタル署名を求める。

【0036】このようにして形成された映像データとそれに対応するデジタル署名は、操作者からの指示に応じて、メモリ部 memory for recorded data に記録されるか、外部装置とのインターフェイス external I/F を介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影して形成されたデジタルデータが一度メモリ部 memory for recorded data に記録された後にデジタル署名生成部 C-CODEC に入力されることもあり得る。

【0037】以上のような映像入力装置において、デジタル署名が生成されるとき具体的な手続きは次のようになる。

【0038】デジタル署名生成

CPU は、外部装置とのインターフェイス external I/F を介して携帯装置から秘密鍵 sk_{aan} とデジタル署名生成アルゴリズム D_{aan} とを映像入力装置内のメモリ部 work memory と CPU とにダウンロードする。次に、映像入力装置内で形成されたデジタル映像データ I を用いて $D_{aan}(sk_{aan}, I)$ を計算し、それをデジタル署名として出力する。そして、このようにして得られる映像データ I とデジタル署名 $D_{aan}(sk_{aan}, I)$ は、メモリ部 memory for recorded data に記録されるか、外部装置とのインターフェイス external I/F を介して外部装置に送られるか、あるいはその両方が行なわれる。

【0039】また、映像データとそれに対応するデジタル署名とが確かに上記の携帯装置が接続されたときに入力された映像であるか否かを検証する具体的な手続きは、以下になる。

【0040】デジタル署名検証

記録データ（映像データ I' とデジタル署名 $D'_{aan}(sk_{aan}, I)$ とする）を受け取った検証者は、デジタル署名検証アルゴリズム E_{aan} と公開鍵 pk_{aan} とを用いて、 $I' = E_{aan}(pk_{aan}, D'_{aan}(sk_{aan}, I))$ が成り立つかどうかを確認する。

【0041】ここで、上式が成立した場合は、記録デー

タの映像 I' は上記携帯装置が接続されたときに撮影された映像 I である。一方、上式が成立しない場合は、記録データの映像 I' が上記携帯装置が接続されたときに撮影された映像 I ではない映像になっている。すなわち、 $D'_{aan}(sk_{aan}, I)$ の値が $D_{aan}(sk_{aan}, I)$ の値とは異なる、あるいは映像データ I' とデジタル署名 $D'_{aan}(sk_{aan}, I)$ との両方が異なる、のいずれかの場合であり、上記携帯装置が接続されたときに撮影された映像データではないと判断することができる。

【0042】したがって、このような映像入力システムにおいて、携帯装置が撮影者と正確に一对一に対応していれば、撮影者が撮影した映像であることを保証するシステムが実現できる。

【0043】〔第3の実施形態〕本実施形態では、デジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置に接続される外部装置に固有の秘密情報として公開鍵暗号の秘密鍵を有するとともに、その携帯装置が演算能力を持ち、デジタル署名生成の手続きを以下のように行う場合について、図1を用いて説明する。

【0044】デジタル署名生成

CPUは、映像入力装置内で形成されたデジタル映像データ I を、外部装置とのインターフェイス external I/F を介して携帯装置に送る。携帯装置は、その内部に記憶されている秘密鍵 sk_{aan} とデジタル署名生成アルゴリズム D_{aan} とを用いて、送られて来た映像データ I からデジタル署名 $D_{aan}(sk_{aan}, I)$ を計算し、それを外部装置とのインターフェイス external I/F を介して映像入力装置に送る。

【0045】そして、このようにして得られた映像データ I とデジタル署名 $D_{aan}(sk_{aan}, I)$ は、メモリ部 memory for recorded data に記録されるか、外部装置とのインターフェイス external I/F を介して外部装置に送られるか、あるいはその両方が行なわれる。

【0046】デジタル署名検証

第2の実施形態と同じであるので、説明を省略する。

【0047】〔第4の実施形態〕本実施形態では、デジタル署名アルゴリズムとして公開鍵暗号を用い、映像入力装置とその外部装置である携帯装置との両方がそれぞれ固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図1を用いて説明する。なお、本実施形態の処理は、以下のデジタル署名生成と検証の処理を除いて、第1の実施形態および第2の実施形態と同じである。

【0048】デジタル署名生成

CPUは、外部装置とのインターフェイス external I/F を介して携帯装置から秘密鍵 sk_{aan} とデジタル署名生成アルゴリズム D_{aan} とを映像入力装置内のメモリ部 work memory とCPUとにダウンロードする。次に、上記映像入力装置内で形成されたデジタル映像データ I

から $D_{aan}(sk_{aan}, I)$ を計算し、その計算結果をデジタル署名生成部 C-CODEC に入力する。

【0049】デジタル署名生成部 C-CODEC は、入力されたデータ $D_{aan}(sk_{aan}, I)$ に対し、 $D_{can}(sk_{can}, D_{aan}(sk_{aan}, I))$ の計算を実行し、その計算結果をデジタル署名として出力する。このようにして形成された映像データ I とデジタル署名 $D_{can}(sk_{can}, D_{aan}(sk_{aan}, I))$ とは、メモリ部 memory for recorded data に記録されるか、外部装置とのインターフェイス external I/F を介して外部装置に送られるか、あるいはその両方が行なわれる。

【0050】また、映像データとそれに対応するデジタル署名とが確かに上記携帯装置が接続されたときに上記映像入力装置で入力された映像であるか否かを検証する具体的な手続きは、以下になる。

【0051】デジタル署名検証

記録データ（映像データ I' とデジタル署名 $D'_{can}(sk_{can}, D_{aan}(sk_{aan}, I))$ とする）を受け取った検証者は、映像入力装置に固有のデジタル署名検証アルゴリズム E_{can} と公開鍵 pk_{can} 、および携帯装置に固有のデジタル署名検証アルゴリズム E_{aan} と公開鍵 pk_{aan} を用いて、

$$I' = E_{aan}(pk_{aan}, E_{can}(pk_{can}, D'_{can}(sk_{can}, D_{aan}(sk_{aan}, I))))$$

が成り立つかどうかを確認する。

【0052】ここで、上式が成立した場合は、記録データの映像 I' は上記映像入力装置で上記携帯装置が接続されたときに撮影された映像であるが、上式が成立しない場合はそれとは異なる映像であると判断することができる。

【0053】なお、上記の実施形態では、デジタル署名生成の順序は、最初に携帯装置で次に映像入力装置の順であったが、逆にすることも可能であり、その場合は検証の順序も逆になる。また、映像入力装置と携帯装置との両方が署名したデータをその順序にかかわらず生成、検証することも可能である。さらに、携帯装置のデジタル署名生成アルゴリズム D_{aan} を映像入力装置の内部に記憶しておき、秘密鍵 sk_{aan} のみを携帯装置に記憶しておくこともできる。

【0054】〔第5の実施形態〕次に、圧縮技術を用いて、記録する映像データの代わりにそれを圧縮したデータに対してデジタル署名を生成する場合について説明する。ここでは、圧縮変換を c で表すこととする。映像データの正当性を確認するエンティティ（検証者と呼ぶ）は、この圧縮変換 c を知っている。その他は、上記第1～第4の実施形態と同様である。

【0055】デジタル署名生成

CPUは、映像入力装置内の撮像部 imaging method で形成されたデジタル映像データ I に対し $c(I)$ の計算を実行し、それにより得られる圧縮データ $c(I)$ を映

像データIの代わりに用いる。他の処理は、上記第1～第4の実施形態と同様である。例えば、第1の実施形態の場合に即して説明すると、映像データIとデジタル署名 $D_{can}(sk_{can}, c(I))$ とがメモリ部memory for recorded dataに記録されるか、外部装置とのインターフェイスexternal I/Fを介して外部装置に送られるか、あるいはその両方が行なわれる。

【0056】デジタル署名検証

記録データ(映像データI'とデジタル署名 $D'_{can}(sk_{can}, c(I))$ とする)を受け取った検証者は、デジタル署名検証アルゴリズム E_{can} と公開鍵 pk_{can} とを用いて、

$$c(I') = E_{can}(pk_{can}, D'_{can}(sk_{can}, c(I)))$$

が成り立つかどうかを確認する。なお、検証者が圧縮変換の逆変換 c^{-1} を知っているならば、

$$I' = c^{-1}(E_{can}(pk_{can}, D'_{can}(sk_{can}, c(I))))$$

が成り立つかどうかを確認してもよい。

【0057】ここで、上式が成立した場合は、記録データの映像I'は上記映像入力装置で撮影された映像である。一方、上式が成立しない場合は、記録データの映像I'が上記映像入力装置で撮影された映像Iではない映像になっている。すなわち、 $D'_{can}(sk_{can}, c(I))$ の値が $D_{can}(sk_{can}, c(I))$ の値とは異なる、あるいは映像データI'とデジタル署名 $D'_{can}(sk_{can}, c(I))$ との両方が異なる、のいずれの場合であり、上記映像入力装置で撮影、形成された映像データではないと判断することができる。

【0058】〔第6の実施形態〕本実施形態では、映像入力装置の一例としてデジタル・カメラを取り上げ、デジタル署名アルゴリズムとして公開鍵暗号を用い、デジタル・カメラと携帯装置との両方がそれぞれ固有の秘密情報として公開鍵暗号の秘密鍵を有する場合について、図2を用いて説明する。

【0059】デジタル・カメラの構成

図2に示した四角の各ブロックは機能別の構成要素であり、それらを結ぶ線は制御バス及びデータバスを表す。IMGは撮像部であり、対象となる被写体を撮影して電気信号に変換する。PRCは画像処理部であり、上記撮像部IMGで形成された電気映像信号に対して適当な信号処理、A/D変換処理、画像処理、情報源符号化処理等を行ない、デジタル・カメラからの出力となるデジタル・データを形成する。

【0060】CPUは中央演算装置であり、ROMに記憶されている制御ソフトウェアに従い、DRAMを計算用の領域として利用しながら所定の計算を行ない、バスを介してカメラ全体の制御を行なう。上記ROMは読みだし専用のメモリ部であり、制御プログラムや圧縮変換、表示データなどの、カメラの制御に必要な制御ソフ

トウェアを記憶する。上記DRAMは読み書き可能なメモリ部であり、CPUが計算を行なうための作業用に使われる。

【0061】STRGはメモリ部であり、撮影した映像データや音声データあるいはその一部を記録する。CODECはデジタル署名生成部であり、秘密鍵と署名生成アルゴリズムとを記憶しており、これらを用いて、入力されたデジタル・映像データに対するデジタル署名を生成する。

【0062】I/Fは外部装置とのインターフェイス、PCMCIAは外部装置とのPCMCIA規格に基づくインターフェイスであり、本実施形態の映像入力装置は、これらのインタフェースを介して映像データ、制御ソフトウェア、状況データ等をコンピュータやメモリ等の外部装置と通信する。MICは音声入力部であり、音声を収集し電気信号に変換する。OP-SWは操作部、LCDはディスプレイ、LEDはランプであり、これらを用いてユーザは必要な情報の入出力を行い、カメラを操作する。

【0063】このような構成において、映像入力における基本動作は、以下の通りである。すなわち、ある対象を撮影して映像入力を行なうとき、携帯装置はカメラ内の外部装置とのインターフェイスI/Fに接続され、撮影者は、操作部OP-SWから撮影の指示を入力する。

【0064】CPUと携帯装置は、外部装置とのインターフェイスI/Fを介して通信し、携帯装置に記憶されている秘密鍵とデジタル署名生成アルゴリズム、およびカメラ内に記憶されている秘密鍵とデジタル署名生成アルゴリズムを用いて、撮影して形成された映像、音声のデジタル・データを圧縮したデータに対するデジタル署名を求める。

【0065】上記撮影した映像データと録音した音声データとは、操作者からの指示に応じてメモリ部STRGに記録されるか、外部装置とのインターフェイスを介して外部装置に送られるか、あるいはその両方が行なわれる。なお、撮影、録音して形成されたデジタル・データが一度メモリ部STRGに記録された後にデジタル署名が生成されることもあり得る。

【0066】ここで、本実施形態のデジタル・カメラにおけるデジタル署名生成アルゴリズムを D_{can} 、秘密鍵を sk_{can} 、デジタル署名検証アルゴリズムを E_{can} 、公開鍵を pk_{can} とする。上記デジタル署名生成アルゴリズム D_{can} と秘密鍵 sk_{can} は、デジタル署名生成部CODECの内部に記憶されている。また、圧縮変換アルゴリズムhはROMに記憶されている。

【0067】また、携帯装置に収められている秘密鍵を sk_{aan} 、デジタル署名生成アルゴリズムを D_{aan} とし、対応する公開鍵を pk_{aan} 、デジタル署名検証アルゴリズムを E_{aan} とする。上記デジタル・カメラに固有のデジタル署名検証アルゴリズム E_{can} と公開鍵

pk_{cam} 、上記携帯装置に固有のデジタル署名検証のアルゴリズム E_{cam} と公開鍵 pk_{cam} 、および圧縮変換アルゴリズム h は、少なくともデータの正当性を確認するエンティティ（検証者と呼ぶ）には知られている。

【0068】上記のようなデジタル・カメラにおいて、デジタル署名が生成されるとき具体的な手続きは次のようになる。

【0069】デジタル署名生成

CPUは、デジタル・カメラで形成されたデジタル映像及び音声データ I からデータ D_{cam} (sk_{cam} , $h(I)$)を生成し、それを外部装置とのインターフェイス I/F を介して携帯装置に送る。携帯装置は、秘密鍵 sk_{cam} とデジタル署名生成アルゴリズムと D_{cam} を用いて、送られて来たデータ D_{cam} (sk_{cam} , $h(I)$)を用いて D_{cam} (sk_{cam} , D_{cam} (sk_{cam} , $h(I)$))の計算を実行し、その計算結果を、外部装置とのインターフェイス I/F を介してカメラに送る。

【0070】そして、このようにして形成されたデジタル・データ I とデジタル署名 D_{cam} (sk_{cam} , D_{cam} (sk_{cam} , $h(I)$))は、メモリ部STRGに記録されるか、外部装置とのインターフェイスPCMCIAを介して外部装置に送られるか、あるいはその両方が行なわれる。

【0071】また、撮影されたデータとそれに対応するデジタル署名とが確かに上記携帯装置が接続されたときに上記カメラで撮影されたデータであるか否かを検証する具体的な手続きは、以下のようになる。

【0072】デジタル署名検証

記録データ（デジタル・データ I' とデジタル署名 D'_{cam} (sk_{cam} , D_{cam} (sk_{cam} , $h(I)$))とする)を受け取った検証者は、携帯装置に固有のデジタル署名検証アルゴリズム E_{cam} と公開鍵 pk_{cam} 、カメラに固有のデジタル署名検証アルゴリズム E_{cam} と公開鍵 pk_{cam} 、および圧縮変換アルゴリズム h を用いて、

$$h(I') = E_{cam}(pk_{cam}, E_{cam}(pk_{cam}, D'_{cam}(sk_{cam}, D_{cam}(sk_{cam}, h(I))))$$

が成り立つかどうかを確認する。

【0073】ここで、上式が成立した場合は、記録データ I' は上記携帯装置が接続されたときに上記カメラで撮影されたデータである。一方、上式が成立しない場合は、記録データ I' が上記携帯装置が接続されたときに上記カメラで撮影されたデータ I ではないデータになっている。すなわち、 $D'_{cam}(sk_{cam}, I)$ の値が $D_{cam}(sk_{cam}, I)$ の値とは異なる、あるいはデジタル・データ I' とデジタル署名 $D'_{cam}(sk_{cam}, I)$ との両方が異なる、のいずれかの場合であり、上記携帯装置が接続されたときに上記カメラで撮影

されたデータではないと判断することができる。

【0074】〔その他の実施形態〕以上に説明した第1～第6の実施形態の組合せで得られる全ての映像入力装置および映像入力システムは、本発明の対象に含まれる。映像入力装置に加えて検証の手続きも含めた映像入力システムの概念図を、図3に示す。

【0075】図3において、image input deviceは第1～第6の実施形態の映像入力装置、portable deviceは携帯装置であり、これらはexternal I/Fを介して接続されている。また、check deviceはデジタル署名検証処理を実行するための装置、portable device2はportable deviceと同様の携帯装置であり、I/Fを介して接続される。

【0076】例えば、検証装置check deviceは、映像入力装置に固有のデジタル署名検証アルゴリズム E_{cam} と公開鍵 pk_{cam} 、および携帯装置に固有のデジタル署名検証アルゴリズム E_{cam} と公開鍵 pk_{cam} を読み込んだパーソナル・コンピュータ、あるいは、上記デジタル署名検証アルゴリズム E_{cam} と公開鍵 pk_{cam} 、および上記デジタル署名検証アルゴリズム E_{cam} と公開鍵 pk_{cam} を格納した携帯装置portable device2を接続したパーソナル・コンピュータである。

【0077】Imageは撮影の対象であり、映像入力装置が撮影対象Imageを撮影して形成したデジタル映像データが I である。なお、上記携帯装置portable device2と同等の携帯装置portable deviceをexternal I/Fを介して接続した映像入力装置image input deviceが検証装置check deviceとなることも可能である。

【0078】映像データ I は（必要ならば圧縮され、それから）デジタル署名生成部C-CODECおよび外部装置とのインタフェースexternal I/Fを介して携帯装置portable deviceの少なくとも一方に入力されるか、デジタル署名生成部C-CODECとインタフェースexternal I/Fとの間で入出力されるか、あるいはその両方が行われる。

【0079】○印で囲んだ+の記号は、入力を合成する処理を示し、デジタル署名生成部C-CODECおよび携帯装置portable deviceの少なくとも一方からの最終出力と、映像データ I とを合成して出力する。このときの出力形式の例を、図4に示す。図4は、映像データ I とその映像データ I に対するデジタル署名とが連結されてひとまとまりにされている状態である。

【0080】なお、以上の実施形態では、映像データ I とその映像データ I に対するデジタル署名とが出力された。これに対し、RSA暗号のようにデジタル署名から元の情報を復元できるアルゴリズムを用いる場合は、映像データ I が圧縮されていないならばデジタル署名のみを記録するか、外部装置に送るか、あるいはその両方を行えばよい。この場合の例を、図5に示す。また、このときの出力形式の例を図6に示す。

【0081】なお、本発明の対象は、第6の実施形態で述べたデジタル・カメラに限られない。例えば、スキャナ、複写機、ファクシミリ、ファイリング・システム、OCR装置等の映像入力装置に本発明を適用可能であり、それらに対応する検証手段を含めた映像入力システムは、全て本発明の対象に含まれる。また、対象とするデータも映像に限らず、音声、文字情報等の一般的な情報に適用できることは言うまでもない。

【0082】

【発明の効果】以上説明したように、本発明によれば、映像入力装置あるいはそれに接続される外部装置を保持している操作者でないものは映像データに対応するデジタル署名を生成することができず、かつ、出力データに対して改ざんや偽造がなされたときは、上記装置あるいは上記撮影者の公開鍵を用いてそれらを検出するようにシステム全体を構成、運用することが可能になる。

【0083】したがって、その映像データが確かにその映像入力装置で生成された、あるいはその外部装置を保持している操作者によって撮影されたデータだということを保証することが可能になり、デジタル映像データに事実の証拠としての証明能力を与えることができ、用途が限定されてしまう不都合を防ぐことができるようになる。

【図面の簡単な説明】

【図1】本発明の一実施形態である映像入力装置の構成を示すブロック図である。

【図2】本実施形態による映像入力装置の一例であるデジタル・カメラの構成を示すブロック図である。

【図3】本実施形態による映像入力システムの構成例を示すブロック図である。

【図4】出力形式が映像データとデジタル署名との合成である場合のデータの例を示す図である。

【図5】デジタル署名のみを出力する場合の映像入力システムの構成例を示すブロック図である。

【図6】出力形式がデジタル署名のみの場合のデータの例を示す図である。

【符号の説明】

imaging method 撮像部

memory for control program 制御ソフトウェア記憶用のメモリ部

work memory CPUの作業用のメモリ部

operation switch 操作部

motor 機構動作部

memory for recorded data 映像データのメモリ部

external I/F 外部装置とのインターフェイス

C-CODEC デジタル署名生成部

IMG 撮像部

PRC 画像処理部

CPU 中央演算装置

ROM 読みだし専用のメモリ部

DRAM 読み書き可能なメモリ部

STRG 映像データや音声データを記録するメモリ部

CODEC デジタル署名生成部

I/F 外部装置とのインターフェイス

PCMCIA 外部装置とのPCMCIA規格に基づくインターフェイス

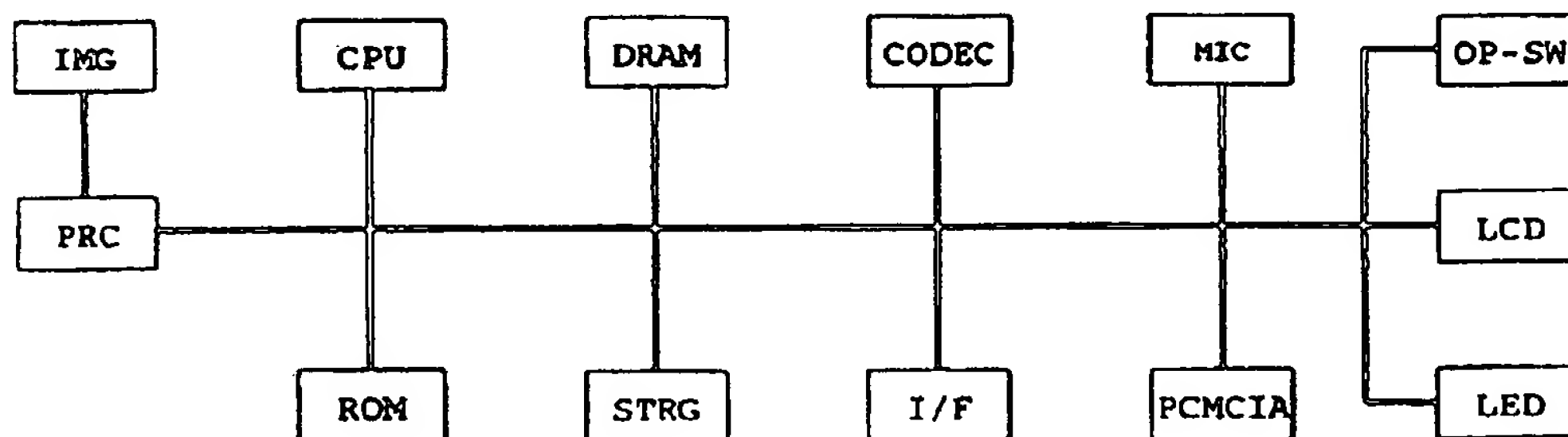
MIC 音声入力部

OP-SW 操作部

LCD ディスプレイ

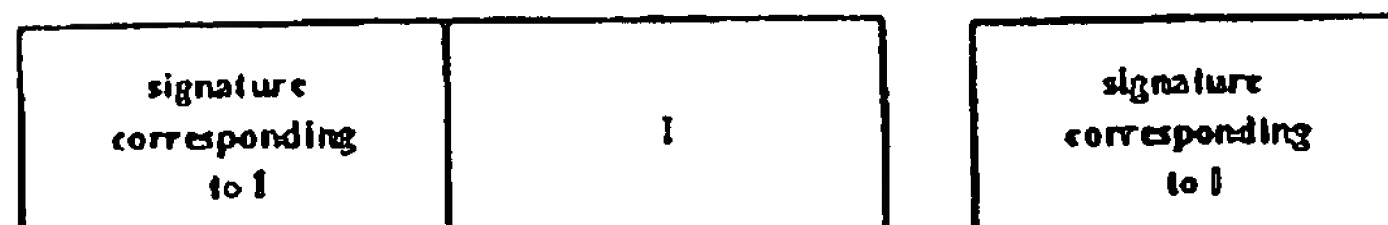
LED ランプ

【図2】

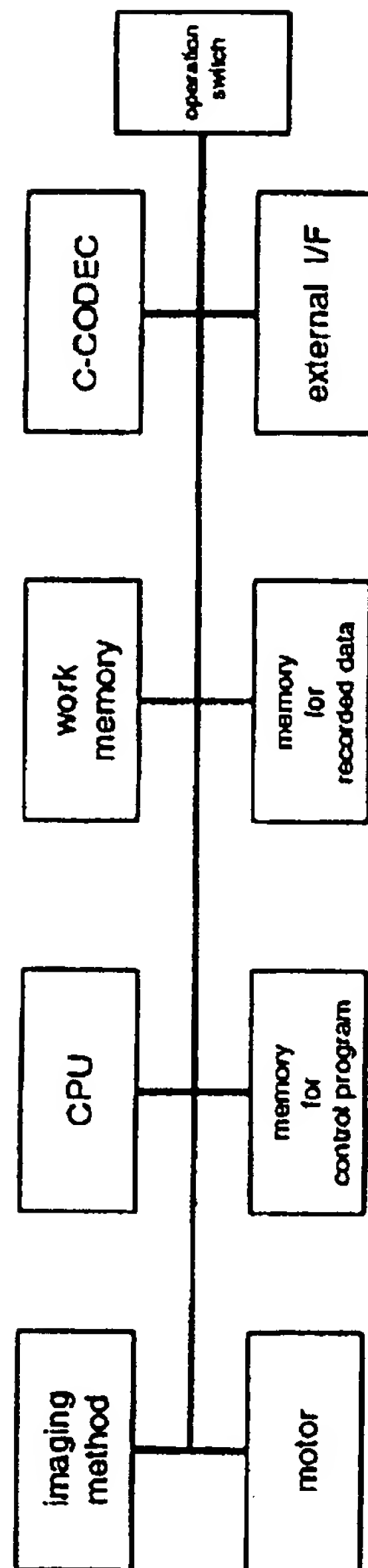


【図4】

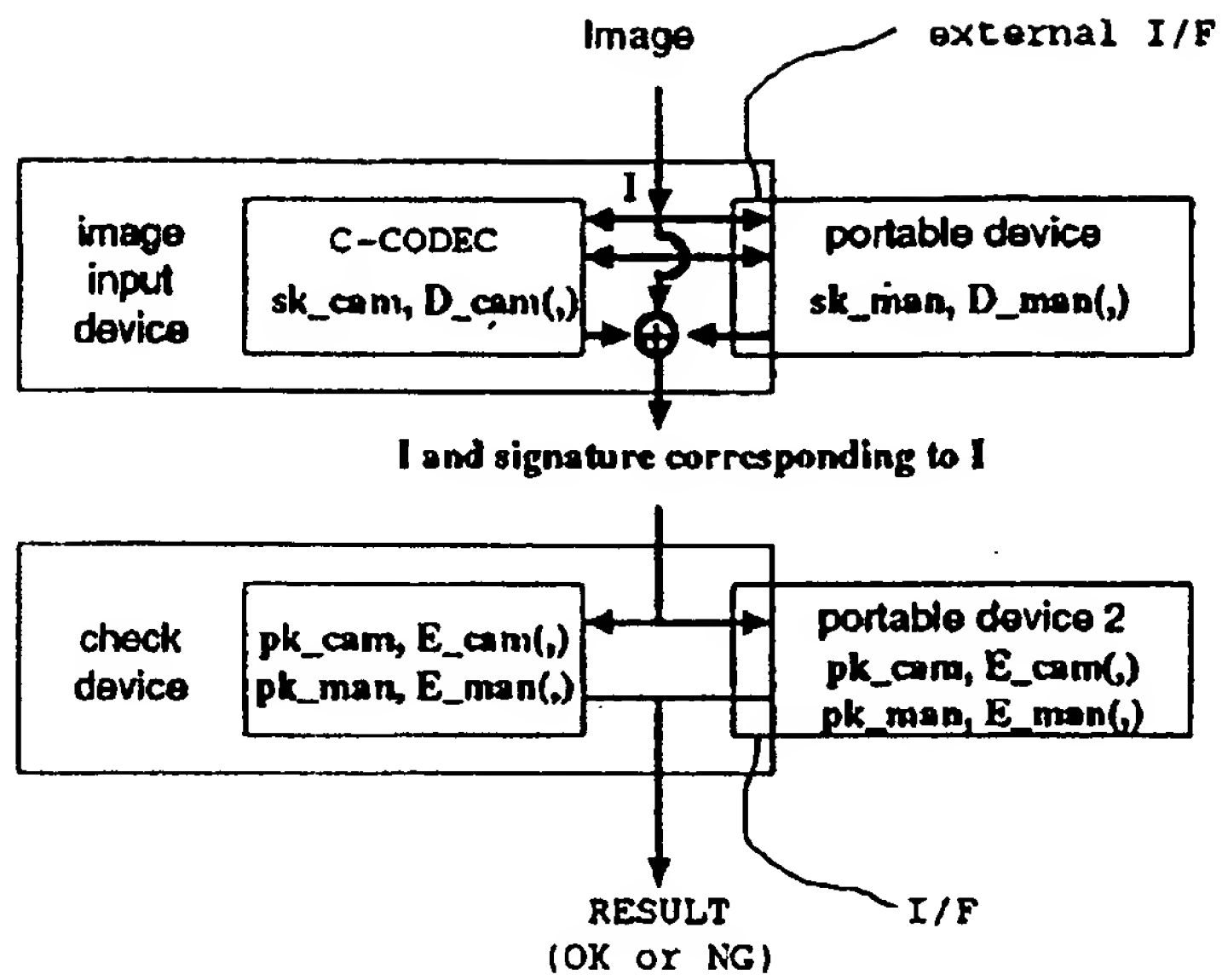
【図6】



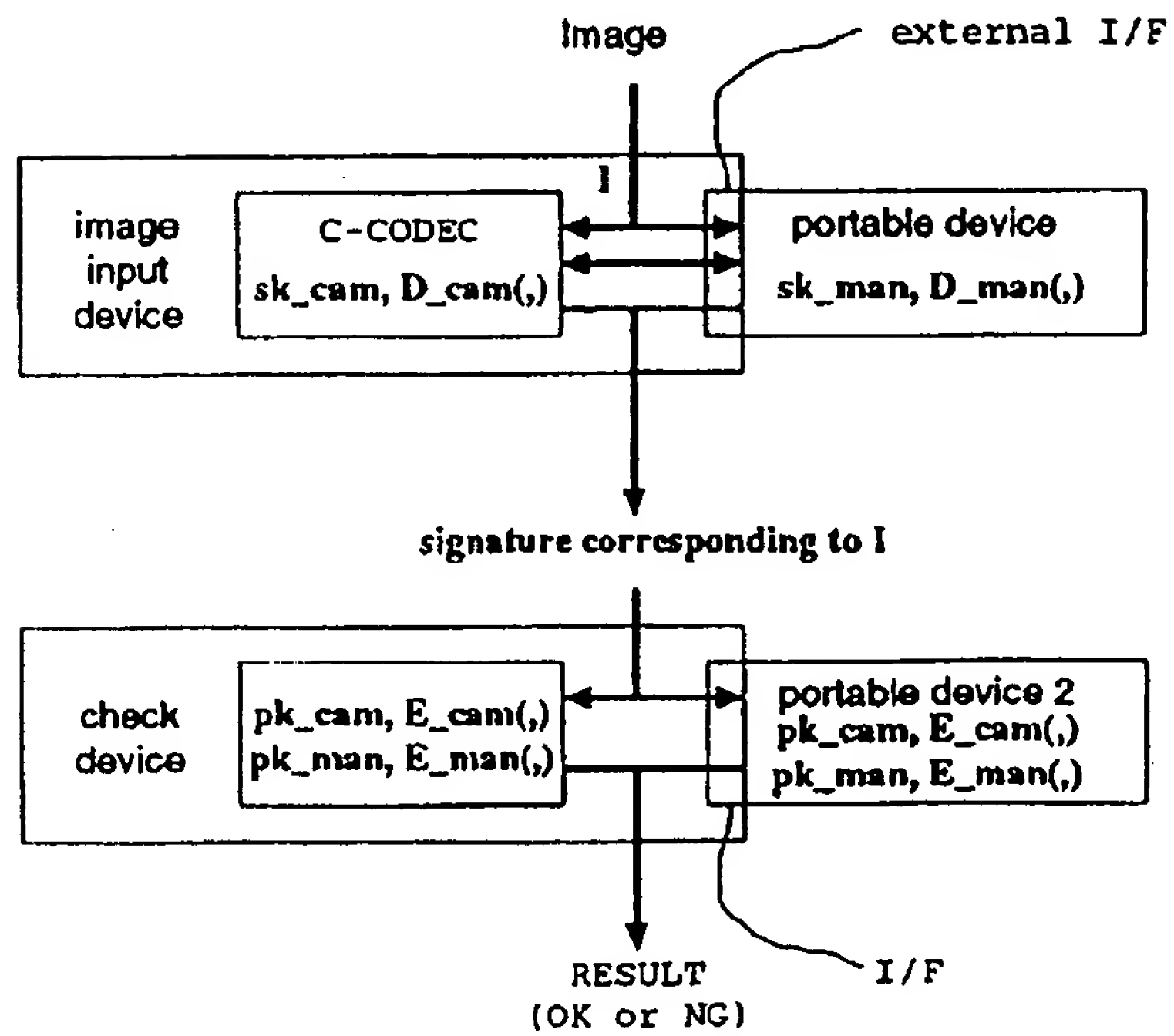
【図1】



【図3】



【図5】



フロントページの続き

(51)Int.Cl.⁶

// H 0 3 M 7/30

識別記号

庁内整理番号

F 1

H 0 4 N 5/91

技術表示箇所

P